UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/809,315	03/24/2004	David M. Durham	42P19299	6493

45209 7590 12/08/2008
INTEL/BSTZ
BLAKELY SOKOLOFF TAYLOR & ZAFMAN LLP
1279 OAKMEAD PARKWAY
SUNNYVALE, CA 94085-4040

EXAMINER	
SCHMIDT, KARI L	

ART UNIT	PAPER NUMBER
2439	

MAIL DATE	DELIVERY MODE
12/08/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/809,315	**Applicant(s)** DURHAM ET AL.
	Examiner KARI L. SCHMIDT	**Art Unit** 2439

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 September 2008*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-38* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-38* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *24 March 2004* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

Notice to Applicant

This communication is in response filed on 09/30/2008. Claims 1-38 are pending.

Response to Arguments

Applicant's arguments, filed 9/30/2008, with respect to the rejection(s) of claim(s) 1-38 under 35 U.S.C. 103 of Baldwin in view of Chen have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Davis in view of Ravi.

Claim Objections

Claim 1 is objected to because of the following informalities: The examiner notes "each client having one of the embedded agents, one embedded agent in each client having an embedded agent" is redundant. Appropriate correction is required.

Claim 5 is objected to because of the following informalities: The examiner notes "with a public and private key associated the client" is missing the linking word to the client (e.g. with/to, etc). Appropriate correction is required.

The examiner further notes other claims (e.g. 2, 23, 29, etc) contain similar redundancies and or informalities that also need correction.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-4, 11, 13-16, 18-20, 22, 24-27, 29, and 30-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Davis et al. (US 2005/0076228 A1) in view of Ravi et al. (US 2005/0204155 A1).

Claims 1, 11, 22, and 29

Davis discloses provisioning a symmetric key across multiple clients through multiple embedded agents (see at least, abstract, [0025]: the examiner notes that a client can consist of a PDA, cellular phone, network-enabled device that is connected to a network and [0029]: the examiner notes a security processor is separate from the host processor and is noted to be the embedded agent and [0074]: the examiner notes the security processor's control processor (e.g. part of the embedded agent) contains symmetric-key encryption), each client having one of the embedded agents, one embedded agent in each client having an embedded agent to store the symmetric cryptographic key in a storage accessible to the embedded agent ([0029]: the examiner notes a security processor is separate from the host processor and acts as the embedded agent and [0074]: the examiner notes the security processor's control processor (e.g. part of the embedded agent) contains symmetric key encryption/decryption) and providing access to encrypted traffic flow in a network to a client if the client is authenticated with the key see at least, [0026]: the examiner notes the secure I/O system performs all network processing and [0048]: the examiner notes the security processor can perform IKE (e.g. internet key exchange is noted as a form of mutual authentication using pre-shared keys (e.g. symmetric, shared, or secret key) between multiple parties). Further Davis discloses that a secure memory not visible to applications and an OS running on the host platform and transparent network link (see at least, [0025]: the examiner notes security processing is segregated from other processing (e.g. protected) and [0026]: the examiner notes the security processing performs all network processing). Further Davis discloses a digital signal processor coupled with the host platform for use in a VPN (see at least, [0025]: the examiner notes a secure I/O allows for a VPN connection and [0030]: the examiner notes an interface may consist of a PHY layer processing (e.g. DSP)).

Davis fails to disclose that the storage accessible to the embedded agent is not directly accessible to a host processor on the client.

However Ravi discloses that the storage accessible to the embedded agent is not directly accessible to a host processor on the client (see at least, abstract: the examiner notes a security processor (e.g. embedded agent) containing a first memory (e.g. storage) that is not accessible to the host processor).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Davis's security processor to include a storage that is not directly accessible to a host processor on the client as taught by

Ravi. One of ordinary skill in the art at the time the invention was made would have been motivated to combine the teachings in order to ensure that the security processor can handle transactions involving accessing protected memory areas (see at least, Ravi, [0050]).

Claim 2 and 30

Davis discloses wherein provisioning the key through the embedded agents further comprises provisioning the key through an embedded agent having network access via a network link not visible to a host operating system (OS) running on the client (see at least, [0025]: the examiner notes security processing is segregated from other processing (e.g. protected) and further this is interpreted to include OS processing and [0026]: the examiner notes the security processing performs all network processing and would also be segregated from the other processing (e.g. OS processing of the client).

Claim 3 and 31

Davis discloses providing access to the traffic flow if the client is authenticated comprises the embedded agent authenticating the client over the network line not visible to the host OS (see at least, [0025]: the examiner notes security processing is segregated from other processing (e.g. protected) and further this is interpreted to include OS processing and [0026]: the examiner notes the security processing performs all network processing (e.g. [0048]: the examiner notes IKE is a form of authenticating over a network) and would also be segregated from the other processing (e.g. OS processing of the client).

Claim 4 and 32

Davis discloses wherein providing access to the traffic flow further comprises providing multiple clients access with the key to nodes in the network, the nodes in the network to decrypt the traffic flow and subsequently encrypt the traffic flow to transmit the traffic to a next node in the network (see at least, [0070]: the examiner notes symmetric key encryption and decryption processing within the security processing system for use in IKE).

Claim 13

Davis discloses wherein the embedded device to have a transparent network link comprises the embedded device to have a network connection not accessible by the host platform, the link to comply with the secure sockets layer (SSL) protocol (see at least, [0025]: the examiner notes security processing is segregated from other processing (e.g. protected) and further this is interpreted to include OS processing and [0026]: the examiner notes the security processing performs all network processing (e.g. [0048]: the examiner notes IKE is a form of authenticating over a network) and would also be segregated from the other processing (e.g. OS processing of the client and [0076]: the examiner notes the use of SSL protocols).

Claim 14

Davis discloses wherein the embedded device to authenticate the apparatus comprises the embedded device to verify the identity of the apparatus to a network switching device with the key, the key to also be used by the network endpoints to verify their respective identities to the network switching device, and the network switching device to decrypt encrypted traffic from the apparatus and the network endpoints (see at least, [0074]: the examiner note IKE and the use of symmetric key encryption and decryption as a forum of authentication of identities between devices).

Claim 15 and 26

Davis discloses wherein the embedded device to authenticate the apparatus comprises the embedded device to hash traffic to be transmitted with the key (see at least, [0069]: the examiner notes a cryptographic core for high-sped encryption and hash processing for packet data).

Claim 16 and 27

Davis discloses wherein the embedded device to authenticate the apparatus comprises the embedded device to perform cryptographic services with the key on traffic to be transmitted (see at least, [0074]: the examiner notes IKE and the use of symmetric key encryption and decryption for traffic to be transmitted).

Claim 18

Davis discloses further comprising a second embedded computation device, the second computation device integrated on the host platform, to verify the security of the host platform (see at least, [0080]: the examiner notes an anti-tamper system is embedded device that contains circuits to check health and integrity of the content in the system).

Claim 19

Davis discloses wherein the first embedded device to not authenticate the apparatus if the second embedded device determines the host platform is not secure (see at least, [0076]: the examiner notes verifying application integrity and [0080]: the examiner notes an anti-tamper system within the security processor checks the integrity of the flash content (e.g. application integrity) and in which it can serve as a trusted device to authenticate another hardware security token connected on (e.g. [0042]))

Claim 20 and 25

Davis discloses further comprising a bi-direction private bus between the first and second embedded device (see at least, [0080]: the examiner notes a the security processor is the first embedded device and contains the anti-tamper system which is the second embedded device and its communication would be private from the host processor (e.g. [0025]: the examiner notes segregated (e.g. private)) and further I/O is a bi-directional bus (eg. [0031])

Claim 24

Davis discloses wherein the embedded chipset comprises an embedded controller agent and an embedded firmware agent, the firmware agent to determine the integrity of the host platform (see at least, [0080]: the examiner notes an anti-tamper system is embedded device that contains circuits to check health and integrity of the content in the system)., and the controller agent to operate the private communication channel and manage access by the host platform to secure network connections (see at least, [0025]: the examiner notes security processing is segregated from other processing (e.g. protected) and further this is interpreted to include OS processing and [0026]: the examiner notes the security processing performs all network processing and would also be segregated from the other processing (e.g. OS processing of the client).

Claims 5 and 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Davis et al. (US 2005/0076228 A1) in view of Ravi et al. (US 2005/0204155 A1). as applied to claim 1 and 29 above, and further in view of Yokota et al. (US 2002/0164035 A1).

Claims 5 and 33

Davis in view of Ravi fails to disclose updating at a client the symmetric cryptographic key provisioned across the multiple clients through a public and private key exchange with a public and private key associated the client.

However Yokota discloses updating at a client the symmetric cryptographic key provisioned across the multiple clients through a public and private key exchange with a public and private key associated the client (see at least, abstract)

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings Davis in view of Ravi to include updating at a client the symmetric cryptographic key provisioned across the multiple clients through a public and private key exchange with a public and private key associated the client as taught by Yokota. One of ordinary skill in the art at the time the invention was made would have been motivated to combine the teachings in order to enable key management center to take the initiative by updated keys or a plurality keys at once thereby conforming to a public key cryptosystem (see at least, Yokota, [0014]).

Claims 6-8 and 34-36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Davis et al. (US 2005/0076228 A1) in view of Ravi et al. (US 2005/0204155 A1) as applied to claim 1 and 29 above, and further in view of Cromer et al. (US 2005/0166213 A1)

Claims 6-8 and 34-36

Davis discloses an embedded agent verifying that a platform associated with the client is not compromised (see at least, [0042]: the examiner notes authenticated another hardware security token to be a platform associated with the client [0076], and [0080])).

Davis in view of Ravi fails to disclose the embedded agent providing the key and an assertion that the client is not compromised to a verification entity on the network.

Cromer an agent providing the key and an assertion that the client is not compromised to a verification entity on the network (see at least, [0048] and [0056]: the examiner notes ensuring the security of the computer system (e.g. verification entity) is not compromised by an unauthorized action by the remote client (e.g. client) and the use of public/private key algorithm to verify the remote client). Further Cromer discloses indicating being compromised and foreclosing network access if being compromised (see at least, [0048] and [0056]: the examine querying the integrity is a form of requesting (e.g. indicating) of being compromised and culminating without further processing is interpreted to be foreclosing).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings Davis in view of Ravi to include the embedded agent providing the key and an assertion that the client is not compromised to a verification entity on the network as taught by Cromer. One of ordinary skill in the art at the time the invention was made would have been motivated to combine the teachings in order to manage a remote client on a computer system in a secure manner by verifying if the OS is not loaded or functioning (see at least, Cromer, [0008]).

Claims 9 and 37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Davis et al. (US 2005/0076228 A1) in view of Ravi et al. (US 2005/0204155 A1). as applied to claim 1 and 29 above, and further in view of Walker et al. (US 2002/0163920 A1).

Claims 9 and 37

Davis in view of Ravi disclose the embedded agent (see claim 1) however fails to disclose further comprising performing cryptographic functions on data with the key to authenticate data with the key.

However Walker discloses performing cryptographic functions on data with the key to authenticate data with the key (see at least, [0012]: the examiner notes a shared key is used to authenticate packets (e.g. data) that are transported)).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings Davis in view of Ravi to include performing cryptographic functions on data with the key to authenticate data with the key as taught by Walker. One of ordinary skill in the art at the time the invention was made would have been motivated to combine the teachings in order to establish confidence that a packet came from the party established by a security association (see at least, Walker, [0012-0013]).

Claims 10, 17, 28, and 38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Davis et al. (US 2005/0076228 A1) in view of Ravi et al. (US 2005/0204155 A1) as applied to claims, 1, 11, 22, and 29, and further in view of Ylonen (US 6,782,474 B1)

Davis in view of Ravi disclose the embedded agent (see claim 1) however fails to disclose further comprising including a derivate of the key in the header of the data to be transmitted to authenticate data with the key.

However Ylonen discloses further comprising including a derivate of the key in the header of the data to be transmitted to authenticate data with the key (see at least, col. 1, lines 56-col. 2, lines 2: the examiner notes a AH is header that contains a computed MAC which is a derivative of the sharked key).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings Davis in view of Ravi to include including a derivate of the key in the header of the data to be transmitted to authenticate data with the key as taught by Ylonen. One of ordinary skill in the art at the time the invention was made would have been motivated to combine the teachings in order to establish implement authentication and security when information travels through the network (see at least, Ylonen, col. 1, lines 34-35 and col. 1, lines 56-co;. 2, lines 2).

Claims 12 and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Davis et al. (US 2005/0076228 A1) in view of Ravi et al. (US 2005/0204155 A1) as applied to claim 11 and 22 above, and further in view of Grohoski et al. (US 2004/0225885 A1).

Claims 12 and 23

Davis in view of Ravi discloses wherein the embedded device to have a transparent network link comprises the embedded device to have a network connection not accessible by the host platform, the link to comply with the secure protocol (see at least, [0025], [0026], [0048], and [0076]).

Davis in view of Ravi fails to disclose wherein the secure protocol is a TLS protocol.

However Grohoski discloses wherein the secure protocol is a TLS protocol (see at least, [0167])

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Davis in view of Ravi to include the use of TLS protocol because as taught by Grohoski. One of ordinary skill in the art at the time the invention was made would have been motivated to combine the teachings in order to provide a processor that can support higher speed encryption and decryption as required by SSL/TLS (see at least, Grohoski, [0056]).

Claim 21 is rejected under 35 U.S.C. 103(a) as being unpatentable over Davis et al. (US 2005/0076228 A1) in view of Ravi et al. (US 2005/0204155 A1) as applied to claim 29 above, and further in view of Kramer et al. (US 2005/0201554 A1).

Davis in view of Ravi fails to disclose further comprising a counter mode hardware cryptographic module on the host platform to encipher traffic with the cryptographic key and further provide a counter mode enciphered of the enciphered traffic.

However Kramer discloses further comprising a counter mode hardware cryptographic module on the host platform to encipher traffic with the cryptographic key and further provide a counter mode enciphered of the enciphered traffic (see at least, [0058] and [0070]).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Davis in view of Ravi to include further comprising a counter mode hardware cryptographic module on the host platform to encipher traffic with the cryptographic key and further provide a counter mode enciphered of the enciphered traffic as taught by Kramer. One of ordinary skill in the art at the time the invention was made would have been motivated to combine the teachings in order to provide encrypting and decrypting data in a network while minimizing interference with future extensions of existing protocols (see at least, Kramer, [0009]).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to KARI L. SCHMIDT whose telephone number is (571) 270-1385. The examiner can normally be reached on Monday - Friday: 7:30am - 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on 571-272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Kari L Schmidt/
Examiner, Art Unit 2439

/Kambiz Zand/
Supervisory Patent Examiner, Art Unit 2434